Data Protection Governance Directive

Document owner	Head of Privacy
Approval	CEO and CFO
Initially adopted	3 September 2018
Date last approved	16 December 2022
Date of next review/approval	Q4 2023
Applicability	Group

Data Protection Governance Directive

1. Introduction

This Group Directive describes how Viaplay Group AB works with data protection from both a governance and material perspective.

2. Target Group

This Group Directive applies to Viaplay Group and to its subsidiaries and controlled entities.

The persons specified in the following table are obliged to read this Directive.

Target Group	Motivation
Members of the Group Executive Management team	Accountable for adherence to the principles set out in this Group Directive and for ensuring allocation of appropriate resources and support.
Members of Function Management teams	Need to know the content of this Group Directive to build a data privacy awareness culture and to ensure allocation of appropriate resources within their respective area.
Head of Privacy and Data Privacy Specialists	Need to know the content of this Group Directive and act in accordance with their defined roles and responsibilities.
All employees in Viaplay Group's Legal and Compliance functions	Need to know the content of this Group Directive and to adhere to the principles set out in this Group Directive and other Group data protection policies and guidelines in their legal advice and decision-making.

3. Definitions

"**Data controller**" – a natural person or legal entity that determines the purposes and means of personal data processing, either alone or jointly.

"**Data protection legislation**" – the EU General Data Protection Regulation (GDPR) and national data protection legislation.

"DPS" – Data Privacy Specialists.

"DPO" – Data Protection Officer.

"General Data Protection Regulation (GDPR)" – EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

"**Joint controller**" – two or more controllers that jointly determine the purposes and means of personal data processing.

"**Personal data**" – any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is an individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, genetic, mental, economic, cultural or social identity of that natural person.

"Personal data breach" – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

"Processor" – a natural person or legal entity that processes personal data on behalf of a data controller.

"Processing" – any operation or set of operations performed on personal data or sets of personal data, including by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Supervisory authority**" – an independent public authority monitoring the application of data protection legislation.

4. Principles

3.1 Viaplay Group's data protection principles

Viaplay Group should be seen as a company that can be trusted and respected for our stance in the field of data protection. It is therefore vital that we adhere to the requirements of the GDPR and other applicable data protection legislation. The protection and processing of personal data at Viaplay Group is based on the principles presented in Viaplay Group's Data Protection Group Policy. Adherence to these principles will help ensure lawful and secure handling of personal data.

3.2 Data protection governance

Viaplay Group is required to implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that processing of personal data is performed in accordance with data protection legislation.

4.1.1. Risks

Unlawful processing of personal data, or a personal data breach, may represent a failure to comply with data protection legislation. This can have very serious consequences for Viaplay Group, including damage to our reputation, loss of trust from stakeholders such as customers, employees, suppliers and regulators, and severe company fines. In some countries, the consequences may also be of a criminal nature and can affect individuals.

4.1.2. Approach

Viaplay Group's approach to data protection is based on the principle of three lines of defence, each with specific ownership, control and assurance responsibilities:

1. The first line of defence is members of the Function Management teams, supported by local DPS's;
2. The second line of defence is the Central Data Protection Team, including Head of Privacy and Heads of IT and Information Security;
3. The third line of defence is Internal Audit.

Viaplay Group has a risk-based approach towards Data Protection. Each function should therefore focus on mitigating immediate/higher risks and ensuring that risks and mitigating actions are appropriately balanced, taking into account the nature, scope, context and purposes of their data processing activities. While Viaplay Group's Privacy Team, consisting of Head of Privacy together with the DPS's, sets the framework for the data protection work, as specified further below, ownership of the privacy risks lies within each function as applicable.

4.1.3. Data Protection & Security Management system (including OneTrust)

Viaplay Group manages a Data Protection & Security Management system that is implemented locally. The system contains information necessary to demonstrate compliance with data protection legislation and related Info & IT Security rules.

As part of this system, Viaplay Group uses OneTrust to map personal data processed within the organisation and to identify data flows within and between Viaplay Group's companies, as well as with third parties. OneTrust also contains information about data processors and the systems used for processing data, the personal data such systems contain and the retention periods for such data. OneTrust is to be updated and supplemented as new processing activities, IT systems or services are developed or procured. Furthermore, Viaplay Group's Consent Management Platform for cookies on various platforms is implemented through OneTrust.

The Data Protection & Security Management system contains (without being limited to), the documentation and information listed below (for some of this information, the OneTrust data mapping inventory system is to be used):

- Information on how Viaplay Group's Data Protection Group Policy and other data protection guidelines are implemented;
- Records of Viaplay Group's Processing Activities and Assets (OneTrust);
- Legitimate Interest Assessments (OneTrust)
- Data Privacy Impact Assessments (OneTrust);
- Records of Viaplay Group's vendors and data processors;
- Information on Data Protection Security requirements (see Viaplay Group's Information Security Group Directive);
- Records of Personal Data Breaches;
- Records of Data Subject Access Requests;
- Annual Data Protection Governance Reports;
- Minutes from Functional Management Team meetings (where data privacy issues are reported);
- Records of Employee Data Protection Training Activities.

4.1.4. First line of defence – function level

a) **Function Management teams**. The Function Management teams of Viaplay Group are responsible for the implementation of, and adherence to, Group data protection policies and directives. They should ensure that data protection principles are followed in day-to-day business activities and processes, and that necessary resources are allocated to be compliant. The Function Management teams shall ensure that Viaplay Group's Data Protection & Security Management system (see 4.2.3) is implemented in their respective area. Appointed DPS's for each functional area need to be able to escalate data protection risks and ask the Function Management teams to take certain decisions. As a result, the Function Management teams shall make sure that data protection is part of their meeting agenda when necessary and at least on a quarterly basis.

b) **DPS's**. Viaplay Group has appointed dedicated DPS's for all its functional areas. The DPS's shall assist specific functions and Head of Privacy in fulfilling the requirements of data protection legislation. DPS's are the primary contact persons for data protection-related topics within their function. They are responsible for advising on, identifying, managing/coordinating and implementing data protection activities within their responsible function, including:

- Raising awareness of data protection issues within their function, including maintenance and deployment of training resources (with assistance from Head of Privacy);
- Implementing Group data protection policies and guidelines;

- Maintaining a record of processing activities (incl. legitimate interest assessment) and systems/assets containing personal data within their functions in OneTrust, including approving new processing activities and systems (in consultation with Head of Privacy);
- Assisting in managing data subject access requests from customers, business partners and employees;
- Supporting the execution of Data Privacy Impact Assessments in OneTrust and consulting with Head of Privacy and related function on mitigation actions (if necessary);
- Assessing whether legislative changes require adaptation of business processes and coordinating any such adaptation (in consultation with Head of Privacy);
- Coordinating audits of third-party processors (when reasonably deemed necessary and in cooperation with Viaplay Group's IT/Information Security teams);
- Assisting stakeholders within the function and legal counsels with negotiations of Data Processing Agreements;
- Reporting and/or Managing Personal Data Breaches within their functions, in collaboration with Head of Privacy and Viaplay Group's IT/Information Security teams;
- Once per year submitting a Data Privacy Governance report (in OneTrust) to Head of Privacy with a summary of all data protection-related activities, GDPR-specific risks, incidents, breaches and mitigation actions, as well as recommendations for follow-up and improvements for their respective function;
- Managing contacts between the local legal entity (i.e. the data controller) and local supervisory authority (in consultation with Head of Privacy);

DPS's should receive appropriate education and training to fulfil these tasks.

4.1.5. Second line of defence – central level

a) **Head of Privacy**. Head of Privacy is Viaplay Group's senior advisor on data protection matters and also hold the role as Viaplay Group's DPO. Head of Privacy is responsible for maintaining Viaplay Group's data protection framework (preparing and updating policies, templates and other guidance documents related to data protection for the Group) and for advising on and monitoring the company's compliance with data protection legislation, Viaplay Group's Code of Conduct and Group policies, and for identifying and coordinating mitigating actions when necessary.

Head of Privacy's responsibilities also include:

- Establishing, deploying and maintaining data protection training activities for Viaplay Group employees;
- Establishing Viaplay Group's annual data protection roadmap, which indicates the main activities on Group level and within the functions for the following year;

- Establishing the yearly Governance wheel setting out the GDPR key stones to be reviewed, updated and maintained throughout the year;
- Serving as a contact point for appointed DPS's and giving advice, recommendations and updates on data protection issues and legislation;
- Advising in relation to new or amended data processing activities;
- Serving as the principal contact point between Viaplay Group and supervisory authorities;
- Updating the Central Data Protection team on relevant developments in the field of data protection;
- Compiling summaries of received data protection reports for the Central Data Protection team, including recommendations for follow-up and improvements;
- Reporting data protection-related risks and issues to Viaplay Group's Audit Committee and the GRC.

Head of Privacy is appointed as a formal DPO for all entities within Viaplay Group and must, in a proper and timely manner, be involved in all issues relating to personal data protection and should be directly accessible for relevant data subjects.

Independence and authority is important for the fulfilment of the DPO role. This means that to exercise the DPO role, Head of Privacy:

- Should perform his/her duties independently and without instruction regarding the exercise of these duties;
- Can request and receive information regarding the processing of personal data without hindrance from management;
- Should have direct access to the highest management level, i.e. in this case Viaplay Group's Audit Committee.;
- Is entitled to address issues to Internal Audit and to the board of directors of legal entities for further investigations;
- Is bound by confidentiality concerning the performance of his/her duties in accordance with the law;
- Should not be instructed, dismissed or penalised by a data controller or data processor for exercising his/her duties;
- Can document and escalate as necessary in the event of objections to his/her guidance;
- Can exercise additional duties, but the organisation should ensure that such duties do not result in a conflict of interests;
- Should receive necessary resources to exercise his/her duties and to maintain expert knowledge in data protection.

b) Central Data Protection team. This team aims to synchronize the data protection work between Head of Privacy and Viaplay Group's IT/Information Security teams. The team also represents a "working committee" that advises on data protection issues

affecting the whole Group. The team's objective is to ensure a uniform Group-wide approach to data protection.

Members of the team include Head of Privacy and Heads of IT and Information Security. Representatives from other business areas and Group functions can be invited when necessary. Meetings should be held when necessary and at least on a quarterly basis.

The Central Data Protection team has the following responsibilities:

- Making decisions on data protection issues that impact the Group or several countries;
- Creating a bridge between data protection and IT/Information Security matters and allocating ownership;
- Escalating major data protection issues (involving high risks and/or extra investments/costs).

4.1.6. Third line of defence – Internal Audit

Internal Audit should ensure that data protection compliance audits are carried out on a regular basis, as well as monitoring fulfilment of Viaplay Group's data protection program and compliance with data protection legislation, Group Policies and Directives.

4.1.7. Relationships between Viaplay Group's legal entities

Functional areas within Viaplay Group do not have any legal rights or obligations under data protection legislation. Such rights and obligations are solely allocated to legal entities.

The legal entities are either to be regarded as data controllers, joint controllers or processors for each process. If one legal entity within Viaplay Group is regarded as a data controller and the other legal entity as a processor, the entities should enter into a data processing agreement, regardless of whether the legal entities are assigned to the same business area. Viaplay Group has intra-Group data processing agreements in place that cover transfer of data between legal entities.

If the entity is a joint controller and has established the purpose and means of data processing together with one or more additional entities, a joint controller arrangement should regulate each entity's responsibility for compliance with data protection legislation.

5. References

- Data Protection Policy
- Information Security Directive

6. Document History and Change Information

For more details of this Group Directive's document history and change information, see Appendix 1.

Appendix 1 – Document History and Change Information

Version	Revision Date	Change Information
1	2018-09-03	Initial Group Directive.
2	2019-12-13	Changes in roles & responsibilities due to internal reorganization. Changes in the governance structure and reporting set-up. Editorial changes.
3	2020-11-26	Deletion of core principles already referred to in Viaplay Group's Data Protection policy, clarifying that the DPO is appointed formal DPO for all entities within Viaplay Group, and minor editorial changes.
4	2022-01-11	Clarified the role of the Central Data Protection Team and also further developed the role of Head of Privacy (previously "Central DPO"). Changed ownership of document to Head of Privacy.
5	2022-09-12	No changes
5.1	2023-06-12	Change from Data Protection Manager (DPM) to Data Privacy Specialist (DPS).